REMARKS

Claims 1-3, 7-19 and 26-30, 32-34, 36 and 38 are pending. Claims 1, 11 and 26 are independent.

Applicant added new claims 39 and 40, depending from claims 11 and 26, respectively, reciting features similar to those recited in claim 33.

The examiner objected to claim 34. Applicant cancelled, without prejudice, claim 34.

The examiner rejected of claims 1-3, 7-19, 32 and 36 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,754,707 to Richards et al., in view of U.S. Patent No. 6,421,732 to Alkhatib et al., and in view of U.S. Patent No. 5,564,070 to Want et al. In addition, the examiner rejected claims 33-34 under 35 U.S.C. §103(a) as being unpatentable over Richards, in view of Alkhatib, in view of Want, and further in view of U.S. Patent No. 6,185,606 to Bereiter. The examiner also rejected claims 26 and 38 under 35 U.S.C. §103(a) as being unpatentable over Richards, in view of Want, rejected claims 27-28 under 35 U.S.C. §103(a) as being unpatentable over Richards, in view of Alkhatib, and further in view of Bereiter, and rejected claims 29-30 under 35 U.S.C. §103(a) as being unpatentable over Richards, in view of Want, and further in view of Alkhatib.

Specifically, responding to applicant's amendments and arguments presented in the Amendment in Reply to Action of June 8, 2006, the examiner stated:

> 2.1 Applicant's remarks, pages 7-12, filed on 8/8/2006, with respect to the rejection of claims 11 and 53 have been fully considered, but they are not persuasive. Applicant argues that Richards fails to teach "establishing a first session between the source computer system and a forwarder/relay service wherein establishing the first session includes processing data to represent the data using a proxy network protocol so that the processed data is configured to tunnel through the first connectivity barrier" as amended. Applicant adds that Richards does not provide any detail regarding processing. It is noted that the independent claims as amended provide no details about the processing by merely stating processing data to represent data so that the data is configured to go through the firewall. The claims as amended do not explicitly recite how the data is processed and what kind of processing is done. Examiner asserts that Richards discloses providing service to clients that cannot normally communicate to each other through the firewall (connectivity barrier) using network protocol TCP/IP, the nexus allows these clients to communicate through a secure connection where communications are sent and relayed to the appropriate client (see

> column 4, line 63- col. 5, line 10). Richards discloses the client resides behind a first connectivity barrier to establish communication with the nexus (forwarder/relay service). The nexus supports network protocol SSL and other encryption process, the SSL provides data encryption, server authentication, message integrity and client authentication for a TCP/IP connection (see column 5, lines 48-64). Therefore as interpreted by the Examiner when an SSL session is established between the client (behind a first connectivity barrier) and the nexus, the client is authenticated using TCP/IP and encryption protocols to establish a secure communication with the nexus, which meets the recitation of processing data using a network protocol to tunnel through the firewall. (See also column 6, lines 52-67 for another embodiment for handling client communication processing between the client and the nexus). In response to Applicant that Alkatib does not disclose a firewall, the gateway of Alkatib is used as a firewall (see column 1, lines 30-33) and meets the recitation of firewall as it controls access to the private network (see column 2, lines 3-8). The mapping disclosed by Alkatib meets also the recitation of processing data as explained in the rejection below. (Office Action, pages 2-3)

Applicant has amended claim 1 to recites "establishing a first session between the source computer system and a forwarder/relay service, wherein establishing the first session includes representing data of a first application in a format associated with a proxy protocol configured to communicate data corresponding to another application so that the data of the first application is communicated through the first connectivity barrier using the proxy protocol."

Support for this feature is provided throughout the filed application, including, for example, at page 7, line 12, to page 8, line 9. Applicant similarly amended independent claims 11 and 26.

As explained in the originally filed application:

> **In addition, the S/FT layer 43 establishes a firewall traversing session, or tunneling session, that allows data communication between the source endpoint 5 and the IP forwarder/relay service 15. The S/FT layer 43 automatically determines the appropriate proxied protocol, such as HTTP, FTP or SOCKS4/5, to use to tunnel application data through a firewall. (page 7, lines 12-18 of the originally filed application)**

Applicant's method enables application data to be sent to the forwarder/relay service through an available firewall proxy(s) by representing the data in a format associated with one of available proxy network protocols corresponding to respective network applications. By representing data of a particular network application that could not otherwise be communicated

over a connectivity barrier in a format corresponding a proxy protocol of some other application (e.g., the proxy protocol for HTTP proxy server, as described on page 1, lines 12-17 of applicant's application) the application data being processed can effectively be "tunneled" through that barrier.

In contrast, none of the cited references describes the feature of "establishing a first session between the source computer system and a forwarder/relay service, wherein establishing the first session includes representing data of a first application in a format associated with a proxy protocol configured to communicate data corresponding to another application so that the data of the first application is communicated through the first connectivity barrier using the proxy protocol."

As explained in applicant's previous Amendment in Reply, Richards describes a secure computer system that includes a central computer (referred to as a "nexus") that facilitates communication between two or more client software programs across wide area networks, including the Internet, where they would normally not be able to communicate with each other (col. 4, lines 55-62). To enable communication between two such client programs, Richards uses a communication link called an upspout, which is a communication link from one of the software clients to the nexus through which the client can send information. The nexus also uses downspouts which are communication links from the nexus to the clients through which the nexus sends information (including data, as well as statistical and control information) to the clients (col. 5, lines 11-30). For example, as Richards explains:

> **To communicate with the client 130, the client 120 sends an upspout 126 through its send communication module 124. The information relayed through the upspout 126 is handled by the nexus incoming communications module 114. The incoming communication module 114 in turn relays the message transmitted by the client 120 through the downspout 128. (FIG. 1, and col. 5, lines 24-30)**

Richards also describes that:

> **The nexus 110 also supports secure communication using the Secure Socket Layer (SSL) protocol, which is an industry standard protocol, and other suitable encryption processes.**
>
> **The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a**

> **TCP/IP connection. SSL comes in two strengths, 40-bit and 128-bit, which refer to the length of the "session key" generated by every encrypted transaction. The longer the key, the more difficult it is to break the encryption code. Most software supports 40-bit SSL sessions, and the latest browsers, including Netscape Communicator 4.0, enable users to encrypt transactions in 128-bit sessions. The secure communications ensures that only the destination client can receive and interpret the communication. No other computer can interpret the data sent from the originating client. (col. 5, lines 48-64)**

While Richards uses an intermediate service (i.e., the nexus) that can support secured communication to form a communication link between two clients, at no point does Richards describe that data of one application is represented in a format associated with the proxy protocol that is configured to communicate data of another application. Thus, Richards fails to disclose or suggest at least the feature of "establishing a first session between the source computer system and a forwarder/relay service, wherein establishing the first session includes representing data of a first application in a format associated with a proxy protocol configured to communicate data corresponding to another application so that the data of the first application is communicated through the first connectivity barrier using the proxy protocol," as required by claim 1.

Alkhatib describes an IPNet Gateway that maps multiple servers on a private IP network to a single IP address on the Internet. However, Alkhatib neither describes nor suggests using an intermediary system, such as a forwarder/relay service. Alkhatib also neither describes nor suggests establishing a communication link between a computer and such an intermediary system nor establishing a communication link where a connectivity barrier (e.g., a firewall) exists between the computer and the intermediary system. Alkhatib does not represent application data in a format associated with a proxy protocol corresponding to another application to communicate data over the connectivity barrier. Therefore, Alkhatib neither describes nor suggests at least the features of "establishing a first session between the source computer system and a forwarder/relay service, wherein establishing the first session includes representing data of a first application in a format associated with a proxy protocol configured to communicate data corresponding to another application so that the data of the first application is

communicated through the first connectivity barrier using the proxy protocol," as required by claim 1.

Want describes a system for maintaining processing continuity in a network having a network accessible application and an intermittently connected wireless system (Abstract). Particularly, as shown in FIG. 3, and as described in col. 4, line 63 to col. 5, line 4:

> **Each mobile computer in the workplace environment is assigned at least one agent. The agent operates primarily for the benefit of its assigned computer. For example, agents are responsible for "knowing" the location of their assigned computers. All communications routed to and from a mobile computer goes through its agent. As the mobile computers in the present invention run applications on remote hosts, all communications between the mobile computer and its applications are mediated by its agent.**

While Want describes that data communicated from the mobile units to their agents include packets (see, for example, cols. 9 and 10), and that such communications may be based on User Datagram Protocol (see col. 10, lines 5-7), nowhere does Want describe that data of a first application is represented in a format associated with a proxy network protocol configured to communicate data corresponding to another application so that the data of the first application can be communicated through a connectivity barrier. Indeed, Want does not describe connectivity barriers and thus Want's system would not represent data so that data could be communicated through connectivity barriers. Accordingly, Want does not disclose or suggest at least the features of "establishing a first session between the source computer system and a forwarder/relay service, wherein establishing the first session includes representing data of a first application in a format associated with a proxy protocol configured to communicate data corresponding to another application so that the data of the first application is communicated through the first connectivity barrier using the proxy protocol," as required by claim 1.

Because none of the references cited by the examiner discloses or suggests, alone or in combination, at least "establishing a first session between the source computer system and a forwarder/relay service, wherein establishing the first session includes representing data of a first application in a format associated with a proxy protocol configured to communicate data corresponding to another application so that the data of the first application is communicated

through the first connectivity barrier using the proxy protocol," applicant's independent claim 1 is therefore patentable over the cited art.

Claims 2-3 and 7-10 and 32-33 depend from independent claim 1, and are therefore patentable over the cited art for at least the same reasons as independent claim 1.

Independent claim 11 recites "establishing a session between the source computer system located behind a first connectivity barrier and a forwarder/relay service, wherein establishing the session includes representing data of a first application in a format associated with a proxy network protocol configured to communicate data corresponding to another application so that the data of the first application is communicated through the first connectivity barrier using the proxy network protocol." Accordingly, for reasons similar to those provided with respect to independent claim 1, at least these features are not disclosed by the cited art. Applicant's independent claim 11 is therefore patentable over the cited art. Claims 12-19, 36 and 39 depend from independent claim 11 and are therefore patentable for at least the same reasons as independent claim 11.

Claim 26, which the examiner rejected under 35 U.S.C. §103(a) as being unpatentable over Richards, in view of Want, recites "wherein the first computer system is configured to represent data of a first application in a format associated with a proxy network protocol configured to communicate data corresponding to another application so that the data of the first application is communicated through the first connectivity barrier using the proxy network protocol." For reason similar to those provided with respect to independent claim 1, at least these features are not disclosed by the cited art. Independent claim 26, therefore, is patentable over the cited art.

Claims 27-30, 38 and 40 depend from independent claim 26 and are therefore patentable for at least the same reasons as independent claim 26.

It is believed that all the rejections and/or objections raised by the examiner have been addressed.

In view of the foregoing, applicant respectfully submits that the application is in condition for allowance and such action is respectfully requested at the examiner's earliest convenience.

All of the dependent claims are patentable for at least the reasons for which the claims on which they depend are patentable.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

No fees are believed due. Please apply any other required fees to deposit account 06-1050, referencing the attorney docket number shown above.

Respectfully submitted,

Date: 3/27/02

Denis G. Maloney
Attorney for Intel Corporation
Reg. No. 29,670

PTO Customer No. 20985
Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (617) 542-8906